Section	**IS Security Policies**	05/01/05	-Effective
		04/28/12	-Revised
Policy 2.00	**Security Monitoring**	Information Services	-Author

Introduction

Security Monitoring is a method used to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as the review of:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- Application logs
- Data backup recovery logs
- Help desk logs
- Other log and error files.

Purpose

The purpose of the Security Monitoring Policy is to ensure that Information Resource security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include Audit Compliance, Service Level Monitoring, Performance Measuring, Limiting Liability, and Capacity Planning.

Audience

The TSSWCB Security Monitoring Policy applies to all individuals that are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resource Security.

Definitions

Information Resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM): Responsible to the State of Texas for management of the agency’s information resources. The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency’s Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

Information Security Officer (ISO): Responsible to executive management for administering the information security functions within the agency. The ISO is the agency’s internal and external point of contact for all information security matters.

Local Area Network (LAN): A data communications network spanning a limited geographical area, a few miles at most. It provides communication between computers and peripherals at relatively high data rates and relatively low error rates.

Security Monitoring Policy

- Automated tools will provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:
  - Internet traffic
  - Electronic mail traffic
  - LAN traffic, protocols, and device inventory
  - Operating system security parameters

- The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:
  - Automated intrusion detection system logs
  - Firewall logs
  - User account logs
  - Network scanning logs
  - System error logs
  - Application logs
  - Data backup and recovery logs
  - Help Desk trouble tickets
  - Telephone activity – Call Detail Reports
  - Network printer and fax logs

- The following checks will be performed at least annually by assigned individuals:
  - Password strength
  - Unauthorized network devices
  - Unsecured sharing of devices
  - Software Licenses

- Any security issues discovered will be reported to the ISO for follow-up investigation.

Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of TSSWCB Information Resources access privileges, civil, and criminal prosecution.

Supporting Information

This Security Policy is supported by the following Security Policy Standards

Reference # **Policy Standards detail**

5 Access to, change to, and use of IR must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as each job status change such as: a transfer, promotion, demotion, or termination of service.

6 The use of IR must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of IR utilization, the establishment of effective use, and reporting of performance to management.

16 Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled.

17 All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the agency is protected from damage, monetary or otherwise. Owner and custodian departments must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.

References

Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications